CODESYS Modbus TCP Server - Improper resource management

CODESYS Security Advisory 2026-05

Published: 2026-05-12

Last Change: 2026-05-12

Identifiers, Type and Severity

CVE-2026-35227
CERT@VDE: VDE-2026-042
CODESYS: MODBUS-327

CWE-772: Missing Release of Resource after Effective Lifetime

CVSS v3.1 Base Score: 5.9 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

1 Summary

CODESYS Modbus is an add-on for the CODESYS Development System that provides a fully integrated Modbus protocol stack along with diagnostic capabilities. A flaw in the CODESYS Modbus TCP Server protocol stack library results in a vulnerability. When a Modbus TCP server is configured, this vulnerable protocol stack is downloaded to and executed by CODESYS Control runtime systems.

The vulnerability is caused by a resource management issue in the Modbus TCP server and is only exploitable if a race condition in the connection handling is successfully triggered. Over time, this may exhaust the configured maximum number of connections, potentially preventing new connections from being accepted. Existing connections remain unaffected and continue to operate normally.

This issue affects only CODESYS projects that include a Modbus TCP server configuration.

2 Affected Products

The following product is affected in all versions before 4.6.0.0:
• CODESYS Modbus

3 Impact

Exploitation of this vulnerability may allow an unauthenticated remote attacker to exhaust all available TCP connections in the CODESYS Modbus TCP Server stack running on a CODESYS Control runtime system, thereby preventing legitimate clients from establishing new connections.

4 Remediation

Update the following product to version 4.6.0.0.
• CODESYS Modbus

To make the fix effective for existing CODESYS projects, you must additionally update the local Modbus TCP Server in the device tree to the latest version and perform a download of the CODESYS application to the PLC.

The CODESYS Development System and the products available as CODESYS add-ons can be downloaded and installed directly with the CODESYS Installer or be downloaded from the CODESYS Store. Alternatively, as well as for all other products, you will find further information on obtaining the software update in the CODESYS Update area https://www.codesys.com/download/.

5 General Security Recommendations

As part of a security strategy, CODESYS GmbH strongly recommends at least the following best-practice defense measures:

• Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside

• Use firewalls to protect and separate the control system network from other networks

• Activate and apply user management and password features

• Limit the access to both development and control system by physical means, operating system features, etc.

• Use encrypted communication links

• Use VPN (Virtual Private Networks) tunnels if remote access is required

• Protect both development and control system by using up to date virus detecting solutions

For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper.

6 Acknowledgments

Reported by ABB Schweiz AG.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

7 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact CODESYS support.

8 Disclaimer

9 Bibliography

[1] CERT@VDE: https://cert.vde.com
[2] CODESYS GmbH: CODESYS Security Whitepaper
[3] CODESYS GmbH: Coordinated Disclosure Policy
[4] CODESYS GmbH download area: https://www.codesys.com/download
[5] CODESYS GmbH security information page: https://www.codesys.com/security
[6] CODESYS GmbH support contact site: https://www.codesys.com/support
[7] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[8] Common Weakness Enumeration (CWE): https://cwe.mitre.org
[9] CVSS Calculator: https://www.first.org/cvss/calculator/3.1

The latest version of this document can be found here:

https://api-www.codesys.com/fileadmin/user_upload/CODESYS_Group/Ecosystem/Up-to-Date/Security/Security-Advisories/Advisory2026-05_MODBUS-327.pdf

Change History

Version	Description	Date
1.0	Initial version	2026-05-12